The Role of Internet in the War against Terrorism – Threatening Privacy or an Ensuring Mechanism (National) Security – the Slovene Perspective

Svete, Uroš

Veröffentlichungsversion / Published Version
Zeitschriftenartikel / journal article

The Role of Internet in the War against Terrorism – Threatening Privacy or an Ensuring Mechanism (National) Security – the Slovene Perspective

Uroš Svete

Abstract: *The use of information-communication technology (ICT) undoubtedly leads towards greater decentralization and individualization of societies. On the other hand, due to the use of ICT, the perception of physical reality has basically changed. When the ICT (security) implications of individual (human) or national security theoretical and empirical perspectives are discussed, a very interesting turning point can be observed. After 11 September 2001, and following the terrorist attacks in Europe, the state has been trying to increase control over ICT and especially the Internet. At the same time, civil society, non-governmental organizations and even individuals have been expressing their own security and other interests, expressed in the fight for privacy and individual human rights.*

Although the state reactions against particular security challenges are often disproportionate, we can see very different policies, even within the same security communities such as NATO and the European Union. Meanwhile, some countries have developed very strong mechanisms for controlling ICT and data retention; in others individual privacy and human rights are still respected and untouchable. Nevertheless, the terrorist attacks showed very clearly that telecommunication data retention as well as other control mechanisms could not prevent all kinds of such attacks. They could only be used after security incidents occurred as a means for identifying perpetrators. How much liberty society is prepared to sacrifice in exchange for greater, but in no way absolute, security depends on societal, political and cultural standards.

Key words: ***human security, privacy, national security, intelligence, civil society, virtual community, human information security, data retention, terrorism.***

Preface

The use of information-communication technology (ICT) (the Internet is often perceived as a "symbol" of such technology) undoubtedly leads towards greater decentralization and individualization of societies. Because of ICT use the perception of physical reality is basically changing.[1] When the ICT (security) implications of

[1] As proof, ICT usage for protection against natural and other disasters could be added. The ICT role in times of social crises caused by such disasters, increased enormously in the fields of public information (mobilizing effect), infrastructure support of complex crisis management systems (coordination and crisis communication) as well as disaster simulation. Information-communication technology has become one of the most important instruments in early warning and prevention, as well in mitigating damage

individual (human) or national security theoretical and empirical perspectives are discussed, a very interesting turning point can be observed. After 11 September 2001, and following terrorist attacks in Europe, the state has been trying to increase control over ICT, especially the Internet, for at least two reasons. For the first time the Internet is becoming more and more important as an instrument in the War against Terrorism because of Hacker Intelligence (HACKINT) and Open Source Intelligence data gathering. Secondly, a large amount of propaganda or psychological warfare against terrorism, irrespective of varying definitions, is spread through the Internet by many Western governments. Human security concept supporters, for whom "big brother" has already entered their bedrooms, with the intention of threatening their privacy, have stressed such a development, which is completely unacceptable to Western liberal government. Although the desire to control the Internet is increasing, on the contrary, individual citizens can still use ICT as one of the most important instruments for controlling state and governmental national security institutions (for example, exchanging and spreading information such as the images of Abu Ghraib prison in Iraq, secret CIA flights of prisoners to Europe) as well for spreading knowledge and awareness of threats to individual privacy. But the great dilemma remains: should human freedom (of communication) be maintained as one of the basic cornerstones of Western liberal and democratic society or it should be sacrificed in the name of greater security, when endangered by new kinds of challenges such as new terrorism threats.

Although Slovenia is not directly threatened by terrorist activities, its political élite is bound by a common security and defence policy to its allies in NATO and the European Union. As a result, some supranational security instruments apply in the Slovene legal and political system. One of the most recent examples we would like to present is civil society's reaction to European Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks. Furthermore, because of great pressure from civil society, academics and information technology professionals, Slovenia has joined the group of EU Member States that have made a declaration under Article 15(3) of this Directive to postpone its application to the retention of communication data relating to the Internet, Internet telephony and Internet e-mail, for 18 months. Thus, the dilemma mentioned above is also being faced in Slovene (political) society, and the outcome will not be determined by Slovene citizens. International alliances as well as politics, technology and the international environment are certainly playing a more important and dominant role, and Slovene society has to follow this.

(The tsunami disaster in Southeast Asia in 2004 confirms how the mobilising effect on the global public opinion level was dramatically increased by ICT. Another good example of effecting global public opinion is The Global Disaster Alert and Coordination System – GDACS, that provides near real-time alerts about natural disasters around the world and tools to facilitate response coordination, including news, maps etc. (http://www.gdacs.org).

Contemporary security theory – moving from national and state level to individual human security

The (national) security overview in recent centuries shows the prevalence of two main approaches in particular: the traditional (deterministic) and post-modern (complex). For the first, security is the absence of an external threat, or rather military means should be used for confronting external threats. This approach justifies national security as a legitimate basis for organized violence within or between states, but not in any situation beyond that (Malešič, 2004). The state has a central role in these security debates; on the other hand it ensures its security interests in an anarchic and hierarchical international environment, above all using military means or military power (Waltz, 2000). In this sense a traditional security approach is basically realistic. It prevailed during the Cold War and was a theoretical base for simplistic, but very important explanations of wars, alliances, imperialism, blockades and other significant international issues (Walt, 1998).

The main features of the traditional security concept, developed in the Cold War period and based on the mentioned starting-points, are common security, stable peace and security approaches in the Third World. Although these concepts go beyond this discussion, they have some very important implications for moving attention to security from the state to the individual level. While the common security project was created by political élites, the stable peace concept arose from peace studies, based on Galtung's and Boulding's analyses. In this sense peace could not be regarded as the absence of war but as a state which ensures the requisite conditions of social justice. Therefore Galtung (Bilgin, 2003: 204) differentiates between personal and structural violence. Equally, he distinguishes negative peace, the absence of armed conflicts, from positive peace, the absence of direct (physical) and indirect (structural and cultural) violence. To achieve positive peace the dialogue, cooperation and solidarity between peoples have to be re-established. It is understandable that Galtung and other authors redirected the research focus from the state and military dimension towards individuals and social groups (Bilgin, 2003: 204–205). The next very important course in security studies is presented by the security approaches of the Third World, in which the great attention to the crises and conflicts of the Cold War period is regarded very critically. Meanwhile Western security concepts, based at that time on the top-down principle, were formed in a completely different way; in the Third World bottom-up principle was preferred as a consequence of the decolonization movement, the Palestinian Question, coup d'états etc. Nevertheless, there were some cases of non-violent, bottom-up security principles. This thesis is easily confirmed by Gandhi's non-violent uprising against British colonialists in India (Bilgin, 2003: 205–207).

In the 1960s more complex definitions of national security appeared. According to the liberal and especially the constructivist critical security theory, the focuses and security agenda had moved from the national state level towards non-state actors. But the new security understanding ("new security") acquired significant legitimacy not

until the end of the Cold War, when human beings/individuals as reference objects of security were exposed to the collapse of the static bipolar world order and the influence of globalization (the concept of human security) (Newman, 2001). On the other hand, the legitimacy of discussion about security subjects (whose security?), security emancipation[2] and insecurity dilemmas (butter or guns, individual vs. state/nation etc.), as well as societal/human security and risk society, is increasing significantly. These subjects can be described in terms of social trends, such as growing economic and political inequalities within particular national states as well between them, a lack of natural resources, migration problems, the spreading of intrastate conflicts, undermining of international peace and stability, and technological challenges. These are just some of the agenda-setting[3] or issues a traditional security paradigm is not faced with. Within this framework more complex security definitions should be understood (Bilgin, 2003). Security, whether or not one insists on a distinction between ”hard” and “soft” security, is about more than protecting a country from external threats; security may well include critical infrastructure protection, economic, social security, environmental and human security (Liotta, 2002: 475).

Table 1: Expanded Concepts of Security as social phenomena according to Møller and Liotta

Theoretical Perspective	**Security form**	**Mode of Expansion**		
		Reference object	***Value at risk***	***Sources of threats***
Traditional (realistic)	National security	State	Sovereignty, Territorial integrity	Other states (Non-state actors after Cold War)
Non-traditional + Traditional (Liberal and realistic)	Societal security	Nations, Societal groups, Political groups	National unity, Identity, Quality of life	(States), Nations, Migrants, Allied cultures
Non-traditional (Liberal)	Human security	Individuals, Mankind, human rights, Rule of law	Survival, Quality of life, Human development	State, Globalization, Nature
Non-traditional (Radical)	Environmental security	Ecosystem	Sustainability, stability	Mankind (sources exploitation, wars, environmental pollution)

Source: Møller (2003: 3) and Liotta (2002: 475).

[2] In critical international studies important attention is focused on bringing to the particular security issues or groups, which were kept in the background for years. In the security debate political, national, social, racial and religious emancipation should be stressed.

[3] Agenda-setting is the creation of public awareness and concern of salient issues by the news media. Agenda-setting theory’s central axiom is salience transfer, in other words, the mass media have the ability to transfer importance of items on their mass agendas to the public agenda.

Individuals as the primary reference objects of security – the concept of human security

Assessing the differences between individuals' and governments' security concerns, Booth (1991) argued that individual security should come first. In advancing his case, he made three interrelated points. Firstly, states cannot be assumed to act as providers of security at all times because some are willing to make significant sections of their population insecure in an attempt to secure themselves (governments that violate the human rights of their own people), and others fail to respond to the needs of their citizens (examples of Albania before Operation Alba, Somalia in the 1990s etc.). In other words, the security of the state is not necessarily synonymous with that of the people who live within its physical boundaries. Secondly, even those states that fit the textbook definition of national security by protecting citizens are generally doing so as a means to an end, not as an end in itself. Thirdly, and finally, cultural, historic, political and traditional differences between states (the role of security culture) make them unlikely to engage in a comprehensive approach to security. Indeed, state-based approaches to security do not allow us to examine the insecurities of individuals and communities within state borders, thereby glossing over a range of suffering in security analyses.

Within the framework of human security, information-communication technology (especially the Internet) use would have indirect as well as direct implications. We must mention the instant threats to individual economic prosperity (for instance, the largest commercial bank in Slovenia had some problems with "phishing" and misuse of its e-banking service recently), political and human rights and free expression (filtering and censuring Internet traffic, blocking particular Internet services or websites, individual Internet traffic data retention). In this sense states as well non-state actors or even individuals could be perceived as sources and targets of threats at the same time. Therefore, from the point of view of ensuring security the way of treating the threats is very important at the national (state)[4] and individual level. But in general, these mechanisms depend in particular on society and the state.[5] Of course, without protection efforts and cooperation within national and global civil society and social integration, which lead to the increased possibility of ICT misuse and at the same time suggested possible solutions, the individual cannot feel safe. In the light of this, Deibert (in Rosenau and Singh, 2002: 126–127) mentioned private security as a very important security conception regarding the aforementioned threat to the individual from information-communication technology (mis)use. As part of the debate regarding the threat

[4] These security measures are institutional (establishment of special institutions for public information about ICT misuse, cooperation with and advising software and hardware producers), educational, strategic-developed and coordinating.

[5] Meanwhile numerous liberal-democratic states have established information commissioners (Germany, Switzerland), inspectors (Sweden) or even Ministries: in Slovenia the ombudsman's deputy has responsibility for the protection of personal data.

to privacy we suggest a new term, joining information (private) and human security, "human information security" – human security within information societies.

The crucial indirect information-communication technology role within the framework of human security is the capacity to share awareness, understanding and knowledge all over the connected world, from the individual to the global community. Without the (digital) media role in security agenda-setting, whenever it presents security issues (threats) or ways of a finding a solution, the human security concept regarding technology could never be functioning and efficient.[6] However, indirectly we also should consider information-communication technology and its role in international humanitarian interventions, one of the most important concrete human security mechanisms. Contemporary international interventions deal with peacekeeping, democratic political process and institution-building in very different types of crises, therefore one organization cannot resolve all security challenges. A very good example is Kosovo, where UN, NGO (non-governmental organizations), OSCE, military and international police are building a network organization called the United Nations Mission in Kosovo – UNMIK. But such a network could not be imagined without information-communication technology use, which ensures a very effective use of resources and a more successful operation and goal achievement. In contrast to traditional, bureaucratic and hierarchical organizations, network organizations are becoming more flexible and adaptable in relation to the environment in which they operate, especially for confronting and managing unexpected threats. But the network organizations are involved with more than just electronic communication. We have to be aware of the limited influence of technology, because it is just a means for achieving goals, and without organizational changes and a new institutional culture such goals could not be achieved. But the most important information-communication technology advantage lies in its reaction capacity and real time data transferring. Nevertheless, the organizational and institutional structure defines how a particular organization would implement new technology solutions (Holohan, 2003).

But even more than for the implementation of peacekeeping operations and humanitarian interventions, with reference to the human security perspective ICT has a key role in new security communities building. Mills (2002) and Rothkopf (1998) argue that virtual security communities should be presented separately. Meanwhile, they

[6] A very good example of how to increase information security awareness is shown by European Digital Rights, which was founded in June 2002. Currently 21 privacy and civil rights organizations from 14 different countries in Europe have EDRI membership. Members of European Digital Rights have joined forces to defend civil rights in the information society. The need for cooperation among European organizations is increasing as more regulation regarding the Internet, copyright and privacy originates from the European Union. Some examples of regulations and developments that attract the attention of European Digital Rights are data retention requirements; spam; telecommunications interception; copyright and fair use restrictions; the cyber-crime treaty; rating, filtering and blocking of internet content; and the notice-and-takedown procedures of websites. European Digital Rights takes an active interest in developments regarding these subjects in all 45 member states of the Council of Europe (http://www.edri.org/).

have qualities for responding to new threats and challenges developing in cyberspace. On the other hand, civil society's organisation of opposition to data retention attempts after the major terrorist attacks in USA and Europe basically confirm this thesis. New (human) security threats, coming from cyberspace, could be countered most effectively only by suitable ICT usage in cyberspace itself. The analysis of how Slovene ICT users built a cyber civil society community and how they have been organizing themselves to protect their rights in terms of privacy and anonymity, will be presented more specifically. This case already shows us that the misunderstanding between individual and national/state (security) interests is becoming greater than ever before. And the interactivity of ICT, the possibility for exchanging ideas beyond state control and territory, is just as crucial, but in no way the only means of protecting individuals.

The Internet and the War against Terror(ism) in Slovenia

Slovene national security policy, including institutions and systems, has been affected by dramatic changes in the last few years. Even though we had to develop a national security system in Slovenia from scratch (the exceptions are the police and in some way civil intelligence), on the other hand the wish to join NATO and European Union (EU) was expressed very quickly, and the transition after entry to both organizations was quite difficult. The Slovene National Security system had to find its own position within a new geostrategic environment, and consideration of the common security policy (the role of Euro-Atlantic organizations) was needed. Taking into account that NATO as well as the EU is founded on a common culture and political values, the more radical Slovene left-wing political élite was forced to redefine some values and principles; on the other hand right-wing parties and intellectuals were and still are very strong NATO and EU supporters, without doubting in both organizations' activities and their (international) policy. After the terrorist attacks and declared War on Terror, connected with the "Coalition of the Willing" invasion of Iraq, the first divisions appeared in Slovene relations with NATO. The left-wing political élite started to express more critical points of view, although Slovenia under a left-centre government signed the Declaration on Joint Cooperation to Counter Terrorism after 11 September. On the other hand, right-wing politics continued to be pragmatic and advocated measures against "rogue states and individuals" suspected of cooperation with terrorist organizations. After the last parliamentary election in 2004, when right-wing parties won and a centre-right coalition was built, former opposition standpoints of uncompromising NATO support became formal. On the other hand, a new opposition and left-oriented media radicalized their antagonism towards US policy in Iraq and also towards the perception and treatment of security issues, prevailing in "New Europe".[7] Following the Slovene government decision to send military instructors to

[7] "New Europe" is a rhetorical term used by conservative political analysts in the United States to describe European post-communist countries. The term implies that there is no single Pan-European identity in the European Union, but that it is divided (and that part of it is "better"). It is a common example of

Iraq and to support the European Parliament and Council proposals on data retention, the political divide in the Slovene public became obvious. The case of data retention and supervising telecommunications was just one in series of events, intensifying the discrepancy between national (state) and individual security efforts.

After the London terrorist attacks European Union member states began to think again about data retention as part of combating terrorism. Just a few days before this tragic event the European Parliament rejected British suggestions for strengthening telecommunication (Internet and mobile telephone traffic) control, but the London terrorist attack again legitimized these attempts. The Slovene Interior Minister made a statement supporting telecommunication data retention as one of the urgent measures and security mechanisms in the fight against terrorism, from the national security perspective of course. It was argued that human privacy would not be affected a result, but mistrust across Europe concerning these data has spread very quickly. Experienced ICT users perceived data retention as a threat to human privacy and security, where state control over its citizens has been increasing dramatically. A major campaign began in cyberspace against data retention and controlling telecommunication, and some Slovene ICT experts as well as the opposition media (for instance *Mladina* weekly) and intellectuals joined the movement. For example, Slovene activists have joined civil society organizations such as Privacy International, European Digital Rights and Statewatch. They have translated the web page *Data Retention is No Solution* (www.dataretentionisnosolution.com/), and made banners and pamphlets. In the second stage of their campaign they informed some Slovene Internet forums, websites and portals. They therefore tried to influence public opinion directly and through electronic and paper media. But the campaign did not stay just at the level of civil society and politics; the opposition against data retention has also been spread to the commercial sphere. Various Slovene Internet providers claimed that the proposed data retention is technically not possible, and on the other hand would cause unacceptable financial and human resources costs. From my point of view it would be exaggerated to claim that these civil society pressures caused the appeasement policy of the Slovene authorities, but the fact is that Slovenia has joined the group of Member States which have declared an 18-month postponement of the application of the Directive on the retention of communication data relating to Internet, Internet telephony and Internet e-mail. Obviously European civil society has had success in some way, thanks above all to the communication capability of the Internet, which ensures coordination among different civil societies at state level. We can say that virtual civil society has become a reality,

the conservative American view of European affairs, and is regarded as an „ignorant" one by many European politicians and many others. „New European" countries were most of all distinguished by their governments' support of the 2003 war in Iraq, as opposed to an „Old Europe" seen as unsupportive of the war. The term Old Europe surfaced in January 2003 after the U.S. Secretary of Defence Donald Rumsfeld used it to refer to European countries that did not support the 2003 invasion of Iraq, most notably France and Germany. It has come to mean a subset of the countries of continental Western Europe(http://en.wikipedia.org/wiki/New_Europe).

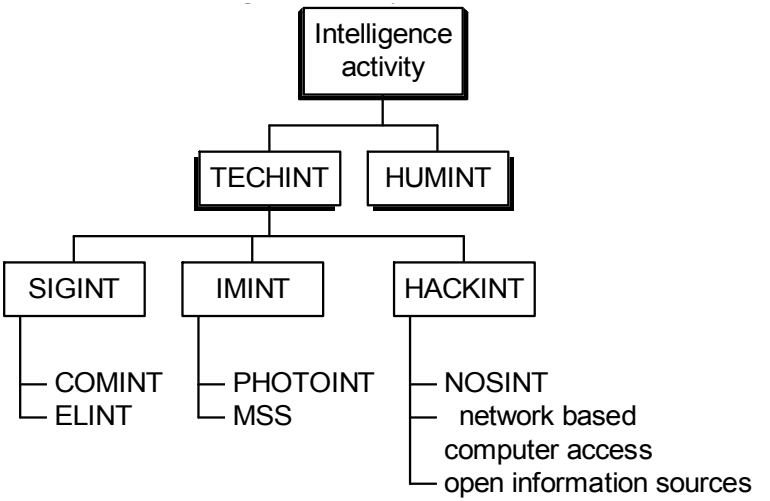
with real political impacts and also interests. The thesis about human (information) security seems to be confirmed or rather, the split between national and human security interests is becoming more obvious. The case is also very significant for authorities, which should, especially within specific technological matters, consider partnership with the private sector (public-private partnership). Without telecommunication companies and experts as well as experienced users support, such a restrictive policy has no choice of succeeding. But the data retention directive is not the only case in Slovenia where individual privacy is threatened from the human security concept point of view. The Slovene government has moved an amendment to the Slovene Intelligence and Security Agency Act. According to it, the time limitation of six months for continual supervision and secret retention of telecommunication data retention should be abolished. The intelligence and security agency accordingly had the theoretical possibility of unlimited encroachment upon someone's communication privacy. The second change is connected with the special/secret use of methods and instruments of the intelligence and security service, which should be controlled and permitted by the Supreme Court president (according to an old legal regulation this was the competence of the district court president). All these attempts have excited curiosity among those opposing the government, in particular the media and experts, and there were accusations that some MPs' e-mails were being intercepted when confidence in intelligence services and government intentions was at its lowest level. The fact is that the growing ICT importance for intelligence data gathering is nothing new (see Figure 1), but on the other hand experienced users are more aware and better organized regarding their protection of privacy rights. The knowledge about state (intelligence) capability for intercepting telecommunications is also spreading very quickly, and is ensured by Internet forums.

In the end we also have to mention ICT use by terrorist organizations for their communication and coordinating activities, psychological warfare, recruitment and fundraising. Extremist and terrorist asymmetric[8] groups have spread propaganda and anti-propaganda through the Internet, as well as coded messages. For such purposes publicly accessible coded software is applied, on the other hand viruses and Trojan horses and other malicious programmes for paralyzing the opponent's information systems are spreading (Kovacich and Jones, 2002). The Iraq case also shows us that information technology and digitalized media have been used for influencing domestic public opinion (for gathering its support) as well for international (especially Western) or global public opinion. This is because Iraqi Islamic groups and some media (Arab information service Al Jazeera) are very skilled in making use of the advantages of information-communication and satellite technologies, and are trying, by showing violence against kidnapped civilians and soldiers, to influence the Western public above all

[8] Asymmetry is warfare where the threats go beyond the enemy's expectations and beyond the readiness of its security mechanism. Therefore, today's terrorism is very often described as contemporary form of asymmetric warfare.

(Rötzer, 2004). Transmitting some forms of violence (beheadings, showing executions directly, and the torture of prisoners) is particularly sensitive for Western civil societies because these images cause upset and anger. Therefore state controlling attempts in the ICT sphere are logical, even in those countries which are not directly threatened by terrorism (such as Slovenia). If modern states want to confront terrorist threats, ICT for intelligence services is indispensable. But for avoiding or minimizing the difference between national and individual security interests, controlling mechanisms should be established and in this sense the role of civil society has to be strengthened. Combating terrorism is not just the matter and interest of a particular national security service, political élite or even ideology, but it should reflect the interests of the society as a whole.

Figure 1: Modern intelligence activity



Source: Davies (1999)

Conclusion

Terrorism is undoubtedly one of the most important threats to modern security efforts. Although the state reactions are often disproportionate (terrorism seems to be more a matter of perception than a matter of reality), we can see very different policies, even within the same security communities, such as NATO and European Union. Meanwhile, some countries have developed very strong mechanisms for controlling ICT and data retention (USA, Great Britain, Italy), in some other countries individual privacy and human rights are still respected and untouchable. The antagonism between "new" and "old" Europe as two separate security communities in NATO and the EU and also between supporters and opponents of the data retention directive, confirms this division. When the mentioned dilemma was faced by Slovene (political) society it became clear that the outcome was not in our hands. Alliances as well as the political

and technological international environment are certainly playing a more important and dominant role. Thus, the Slovene government had just two possibilities: join the group of states that decided in favour of a declaration postponing the Directive implementation or to join the hard-liners in combating terror. Under the pressure of civil society and the Internet community, it decided to join the first group. But nevertheless, the terrorist attacks showed very clearly that telecommunication data retention could not prevent these kinds of attacks. Data retention could just be used afterwards for identifying perpetrators. Thousands of video cameras, the Echelon[9] intelligence system and other data sources undoubtedly confirm that total security can never be achieved.

References

Bilgin, Pinar (2003): Individual and Societal Dimensions of Security. *International Studies Review* 5 (2), pp. 203–222.

Davies, Philip H.J. (1999): The information warfare and the future of the spy. *Information, Communication & Society* 2(2), pp. 115–133.

Holohan, Anne (2003): Cooperation and Coordination in an International Intervention: The Use of Information and Communication Technologies in Kosovo. *Information Technologies and International Development* 1(1), pp. 19–39.

http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/oj/2006/l_105/l_10520060413en00540063.pdf

http://europa.eu.int/eur-lex/lex/LexUriServ/site/sl/oj/2006/l_105/l_10520060413sl00540063.pdf

http://www.mladina.si/tednik/200537/clanek/nar--nove_tehnologije-gregor_cerar/

Kovacich, Gerald, Andy Jones (2002): What InfoSec Professionals Should Know About Information Warfare Tactics by Terrorists. *Computers & Security* 21(2), pp. 113–11.

Liotta, Peter H. (2002): Boomerang Effect: The Convergence of National and Human Security. *Security Dialogue* (33) 4, pp. 473–488.

Malešič, Marjan (2004): Environmental security; a case of Slovenia. In: Mahutova, Katarina – Barich, John J., Kreiznebeck, Ronald A. (eds.). *Defense and the environment : effective scientific communication*, (NATO science series. Series IV, Earth and environmental sciences, vol. 39). Dordrecht; Boston; London: Kluwer Academic Publishers, pp. 139–152.

[9] ECHELON is a name used to describe a highly secretive world-wide signals intelligence and analysis network run by the UKUSA Community (otherwise described as the „Anglo-Saxon alliance“) that has been reported by a number of sources including, in 2001, a committee of the European Parliament (EP report). According to some sources ECHELON can capture radio and satellite communications, telephone calls, faxes, e-mails and other data streams nearly anywhere in the world and includes computer automated analysis and sorting of intercepts. The EP committee, however, concluded that „the analysis carried out in the report has revealed that the technical capabilities of the system are probably not nearly as extensive as some sections of the media had assumed“ (EP report, p. 11)

Mills, Kurt (2002): Cybernations: Identity, Self-determination, Democracy and the ``Internet Effect'' in the Emerging Information Order. *Global Society* 16 (1), pp. 69–87.

Mřller, Bjřrn (2003) National, Societal and Human Security: Discussion –Case Study of the Israel-Palestine Conflict. In Hans Günter Brauch, Antonio Marquina, Mohammad El-Sayed Selim, Peter H. Liotta, Paul Rogers (eds.) *Security and the Environment in the Mediterranean: Conceptualising Security and Environmental Conflicts,* pp.277–288. Berlin: Springer.

Newman, Edward (2001) Human Security and Constructivism. *International Studies Perspectives* 2 (3), pp. 239–251.

Rosenau, James N. in J. P. Singh (eds.) (2002): *Information Technologies and Global Politics: The Changing Scope of Power and Governance.* Albany: State University of New York Press.

Rothkopf, David (1998): Cyberpolitik: The Changing Nature of Power in the Information Age. *Journal of International Affairs* 51(2), 325–359.

Rötzer, Florian (2004): " Terror.net: "Online-Terrorismus" und die Medien". Telepolis, http://www.heise.de/tp/deutsch/special/info/17886/1.html, 18.09.2004.

Walt, Stephen M. (1998): One world, many theories. *Foreign Policy* (Spring 1998), pp. 29–35.

Waltz, Kenneth N. (2000): Structural Realism after the Cold War. *International Security* 25 (1), pp. 5–41.

Uroš Svete *has a PhD in defence studies and is working as a teaching assistant at the Faculty of Social Sciences of the University of Ljubljana. His research and professional efforts focus on military and non-military security threats, in particular information-communication technology as a multi-dimensional security phenomena.*

E-mail: uros.svete@fdv.uni-lj.si